ELSEVIER

Discrete Applied Mathematics 122 (2002) 117–126

DISCRETE APPLIED MATHEMATICS

# Projective planes and congestion-free networks

Charles J. Colbourn

*Department of Computer Science and Engineering, Arizona State University, Tempe, AZ 85287-5406, USA*

Received 28 July 1998; received in revised form 1 September 2001; accepted 27 September 2001

**Abstract**

The design of networks using broadcast media so that every two sites lie on a common link, subject to constraints on the number of links at each site (degree), and the number of sites on each link (link size), is examined. A method proposed by Yener et al. is shown to fail, in general, to achieve the minimum link size for a specified degree constraint. The existence of $(k,n)$-arcs in projective planes is employed to improve upon their results. © 2002 Elsevier Science B.V. All rights reserved.

## 1. Introduction

Yener et al. [29] examine a network design problem and propose an algorithm for constructing scalable, congestion-free network topologies. They assert that their technique provides optimal solutions in terms of degree (number of links at a site) and link size (number of sites on a link). The purpose of this paper is twofold. First, some relevant literature and combinatorial connections are introduced. Secondly, it is shown that the algorithm of Yener et al. [29] can fail to produce optimal solutions.

The network design problem of interest is as follows. There are $n$ network sites, to be connected using multidrop communication links such as Ethernets, token rings, or any broadcast medium. A *link* or *bus* is a subset of the $n$ sites. In order to avoid congestion due to switching overhead from one link to another, it is required that every two sites appear together on at least one link. Typically, each site is equipped with a limited number of communication ports, and hence can appear on at most some fixed number $r$ of the links. Similarly, each link has a limit on the number of sites that it can connect. Reasons for such a limitation include capacity limits, and limits on acceptable routing delay within the link. With these constraints in mind, the problem can be informally stated as follows: connect $n$ sites so that every two sites appear

*E-mail address:* charles.colbourn@asu.edu (C.J. Colbourn).

0166-218X/02/$ - see front matter 
PII: S0166-218X(01)00356-0

together on at least one link, subject to the constraint that no link has more than $k$ sites on it, and no site appears on more than $r$ links.

Problems of this type have been studied extensively. Mickunas [25] considered the case when $k$ and $r$ are close to equal. Subsequently, Bermond and his colleagues [4–6] considered general network design problems of this type under the name "bus interconnection networks". They are primarily responsible for observing that numerous well-studied combinatorial configurations lead to useful solutions to such network design problems (see also [12,21]).

In order to understand the method of Yener et al. [29] and to comment on it, we shall require a number of definitions which are standard in combinatorial design theory [7,10], but not common in the vernacular of network design.

A *set system* of *order* $v$ is a set $V$ of $v$ elements, together with a collection $\mathscr{B}$ of subsets of $V$. Each subset $B \in \mathscr{B}$ is called a *block* or *line*. The set of *blocksizes* is $K = \{|B|: B \in \mathscr{B}\}$, and the set of *replication numbers* is $R = \{|\{B : x \in B \in \mathscr{B}\}| : x \in V\}$. A set system $(V, \mathscr{B})$ is a $\lambda$-*covering* when, for every pair $\{x, y\} \subseteq V$, there are at least $\lambda$ blocks $B \in \mathscr{B}$ with $\{x, y\} \subseteq B$. When $\lambda = 1$, the simpler term *covering* is employed. In this language, the network design problem asks for a covering of order $n$ in which the maximum value in $K$ does not exceed $k$ and the maximum value in $R$ does not exceed $r$.

The construction of coverings in the literature has focussed on the case where every pair is covered precisely $\lambda$ times. Then the covering is termed a $(K, \lambda)$-*pairwise balanced design*, or PBD. When $\lambda = 1$, the simpler notation $K$-PBD is employed. Within this class, if we insist that all block sizes are the same (i.e., $K = \{k\}$), then the PBD is a (*balanced incomplete*) *block design*, or $(v, k, \lambda)$-*design*. Block designs are the central objects of study in combinatorial design theory; see [7] for a detailed text and [10] for a comprehensive handbook. From the given parameters $v$, $k$, and $\lambda$, one can readily determine that all replication numbers are the same value $r = \lambda(v-1)/(k-1)$, and that the number of blocks is $b = \lambda v(v-1)/k(k-1)$.

Block designs and pairwise balanced designs lead to optimal solutions for the network design problem when $k < r$ [4,5]. When $k = r$, a specific class of block designs first explored in finite geometry arises. A block design with $k = r$ and $\lambda = 1$ is a *projective plane*. One can calculate that if $k = r = q + 1$, then $v = b = q^2 + q + 1$, and hence that a projective plane is a $(q^2+q+1, q+1, 1)$-design. This is called a projective plane of *order* $q$; the reuse of the term 'order' unfortunately causes some confusion with the use of 'order' for the number of elements, but the term appears to be firmly entrenched in both usages; context makes the meaning clear.

Projective planes play a central role in the method of Yener et al. [29], and so we provide a brief overview; see [20] for details. A projective plane of order $q$ exists whenever $q$ is a prime or a power of a prime (e.g., when $q = 2, 3, 4, 5, 7, 8, 9, 11, 13, 16$ and so on). Indeed there is a direct construction of a particular plane for each such order from the finite field of order $q$; this plane is often denoted $\mathrm{PG}(2, q)$ and called the *desarguesian projective plane* of order $q$. Projective planes are not known for orders having two distinct prime factors, and the Bruck–Ryser–Chowla theorem (see, e.g. [7,20]) establishes that for certain orders no projective plane can exist. The first two orders excluded are 6 and 14. A large exhaustive computer search established that there is no projective plane of order 10 [22]. However, the general situation for orders that are not powers of a prime is not well understood. Indeed, the existence of projective planes of infinitely many orders remains unsettled, with the smallest open cases being for orders 12 and 15. Although the only planes known have orders that are prime powers, not all known planes are the desarguesian planes from the finite field. Indeed when $q \geqslant 9$ and $q$ is a second or higher power of a prime, there exist more than one projective plane of order $q$. At present, when $q$ is a prime, the only plane known is the desarguesian one.

Desarguesian planes inherit a rich structure from the underlying finite field [18,20]. We introduce one of the known properties of $PG(2,q)$, and introduce further properties later as needed. The desarguesian projective plane of order $q$ can be represented with elements $\mathbb{Z}_{q^2+q+1}$ (the integers modulo $q^2+q+1$), so that whenever $B=\{b_0,\dots,b_q\}$ is a block, so also is $B+1=\{b_0+1,\dots,b_q+1\}$, with all computations in the integers modulo $q^2+q+1$. For each block $B=\{b_0,\dots,b_q\}$, we find that $\{b_i-b_j\colon 0 \leqslant i,j \leqslant q \text{ and } i \neq j\}$, arithmetic modulo $q^2+q+1$, contains every nonzero integer in $\mathbb{Z}_{q^2+q+1}$. Hence, every nonzero difference arises exactly once as the difference modulo $q^2+q+1$ of two elements in $B$. A set with this property is called a *difference set* over $\mathbb{Z}_{q^2+q+1}$. To recover all blocks of the plane, simply add $i$ to each element of $B$ modulo $q^2+q+1$, for each $i \in \mathbb{Z}_{q^2+q+1}$. Some small difference sets are $\{1,2,4\}$ modulo 7 for $q=2$, $\{0,1,3,9\}$ modulo 13 for $q=3$, $\{3,6,7,12,14\}$ modulo 21 for $q=4$, $\{1,5,11,24,25,27\}$ modulo 31 for $q=5$, and $\{1,6,7,9,19,38,42,49\}$ modulo 57 for $q=7$.

## 2. The Method of Yener, Ofek, and Yung

Returning to the network design problem, practical concerns dictate that the replication number $r$ be a fixed small number, while the blocksize $k$ can be potentially much larger than $r$. Since block designs and PBDs always have $k \leqslant r$ by Fisher's inequality [7], a technique is needed to treat cases when $k > r$. This is one of the problems treated in [29].

Bermond et al. [4] propose the following. Suppose that we are to construct a covering with replication number at most $r$ and blocksize at most $k$, and our objective is to maximize the number of elements. Choose $q$ so that $q$ is a power of a prime, $q+1 \leqslant r$, and $q$ is as large as possible subject to these constraints. Then form $PG(2,q)$ on element set $V$ of size $q^2+q+1$, and with block set $\mathscr{B}$. A *weight function* $\omega$ : $V \mapsto \mathbb{Z}^+$ from elements to positive integers is to be chosen, and a set of elements $W=\{(x,i)\colon x \in V \text{ and } 1 \leqslant i \leqslant \omega(x)\}$ defined. The weight of an element indicates the number of times that it is replicated in $W$. One chooses $\omega$ so that the *weight* of block $B$, $\omega(B)=\sum_{x\in B}\omega(x) \leqslant k$, for every $B \in \mathscr{B}$, and defines a new set of blocks

$$\mathscr{D}=\{\{(x,i)\colon x \in B \text{ and } 1 \leqslant i \leqslant \omega(x)\}\colon B \in \mathscr{B}\}.$$

Then $(W,\mathscr{D})$ is a covering with blocksizes at most $k$, replication number $q+1 \leqslant r$, and $\sum_{x\in V}\omega(x)$ elements. Naturally, the problem is to determine $\omega$ so as to constrain the weight of each block to $k$ while maximizing the number of elements. Bermond et al. [4,5] conjecture that the covering with replication number at most $r$, block sizes at most $k$, and the largest number of elements, arises in this manner when $r-1$ is a prime power. It follows from a theorem of Füredi [14] that such a covering can have at most $rk-(r-1)\lceil k/r\rceil$ elements. Now, choosing $\omega$ so that all element weights are as equal as possible subject to the constraint on block weight leads to coverings for which Füredi's bound is achieved infinitely often, and approaches this bound as $k\to\infty$ for fixed $r$ when $r-1$ is a prime power [5,6]. Hence, although there are many potential methods for producing coverings, Füredi's result establishes that the asymptotically optimal coverings arise from replicating elements in projective planes.

Bermond et al. [5,6] do not address the question of finding the largest number of elements in a covering with block size at most $k$ and replication number at most $r$ precisely. Yener et al. [29], however, employ a similar underlying strategy but develop techniques for specifying the weight of each element in the projective plane so as to maximize the number of elements. We introduce their technique next. To produce a covering with $v$ elements, blocksizes at most $k$, and replication number at most $r$, let $S=\{q^2+q+1\colon q+1\leqslant r \text{ and } q \text{ is a prime power}\}$. Thus $S$ consists of the numbers of elements in all known projective planes whose order does not exceed $r-1$. A *scaling formula* is a sequence of integers from $S$, $\alpha_0,\dots,\alpha_t$, for which $\sum_{i=0}^{t}\alpha_i=v$ and $\alpha_i\geqslant\alpha_{i+1}$ for $0\leqslant i<t$.

Yener et al. [29] then choose the desarguesian projective plane on $\alpha_0$ elements to be the *base design* $(V,\mathscr{B})$. They determine weights as follows (in fact, they actually duplicate elements in their method, but it is equivalent). Start with all element weights in $V$ equal to 1. Weights are then increased in $t$ phases. For $1\leqslant i\leqslant t$, within phase $i$ the weights of precisely $\alpha_i$ elements are increased by one, and the weights of the remaining elements left unchanged. We then can concentrate on those elements that are to be replicated within a single phase.

Within each phase, elements are selected in a greedy fashion one at a time. Each selection of an element proceeds by first identifying a set $C_0$ of candidates consisting of those elements not already selected in this phase. The set $C_0$ of candidates is further restricted by defining $C_1\subseteq C_0$ so that $x\in C_1$ whenever $x\in C_0$ and $x$ does not lie on a block whose weight is maximum. It may happen that $C_1=\emptyset$ (i.e., that every element in $C_0$ appears on a maximum weight block); when this occurs, $C_1$ is set equal to $C_0$ since every selection will lead to an increase in the maximum weight of a block. Next the remaining candidates in $C_1$ are restricted further, first by examining for each $x\in C_1$ the *minimum* weight of a block containing $x$. Only those candidates that lie on a minimum weight block among these is retained, to form a smaller set $C_2\subseteq C_1$, of candidates. Finally, among the candidates in $C_2$, one determines for each the *second smallest* weight of a block containing the element; and the final set of candidates $C_3\subseteq C_2$ is chosen to be those elements in $C_2$ whose second smallest block is the least among these. Once the candidate set $C_3$ is identified in this way, an element $x\in C_3$ is selected at random, and the weight of $x$ is incremented.

The main goal of the greedy method is to avoid producing blocks of larger weight than is necessary—hence the restriction to candidates in $C_1$. A secondary goal is to avoid the proliferation of blocks of low weight, as one expects all blocks in an optimal covering to have weights close to equal—hence the restriction to candidates in $C_3$. Yener et al. [29] in their Claim 3 assert that, given a scaling formula, this algorithm (equivalent to their Algorithm 7) "scales the base design with minimum increase in its block size".

An implementation of the algorithm was undertaken. Experiments were then performed with the algorithm using scaling formulas for $r=q+1$ where $q$ is a prime power, and $q^2+q+1 < v < 2(q^2+q+1)$, so that the scaling formula contains only two values—the base design PG$(2,q)$ and one phase of replication. In 2500 trials for each PG$(2,q)$, the algorithm succeeded in finding the minimum as claimed when $q=2,3,4,5$. However, when $q=7$, the algorithm did not perform as expected. For PG$(2,7)$ arising from the difference set $\{1,6,7,9,19,38,42,49\}$ , the trials with $v=57+7$, $57+13$, and $57+21$ fail to produce the same maximum block size each time. With $v=57+7$, for example, the greedy method can select elements $(14,18,5,7,49,10,46)$ for duplication to achieve a maximum blocksize of 11, but can also choose elements $(11,48,42,54,25,30,45)$ to achieve a maximum blocksize of 10. Similarly, with $v=57+13$, one trial chooses $(14,18,5,7,49,10,46,29,6,21,16,50,47)$ to achieve a maximum blocksize of 12, while another chooses

$$(11,48,42,54,25,30,45,49,12,26,1,32,10)$$

to achieve a maximum blocksize of 11. With $v=57+21$, one trial selects

$$(14,18,5,7,49,10,46,29,6,21,16,50,47,35,0,56,31,11,20,13,22)$$

for

maximum blocksize 13, while another chooses

$$(55,43,35,5,23,7,0,38,34,46,14,37,1,44,3,19,48,24,26,11,17)$$

for maximum blocksize 12.

One concludes that the algorithm proposed does not in fact guarantee the minimum increase in the blocksize, even when the scaling formula is fixed. Experiments with larger projective planes confirm this, and hence it appears that only in planes of very small order is the greedy method proposed sufficient to ensure minimum increase in the blocksize.

One might hope that, while not guaranteeing the minimum increase in the maximum blocksize, the algorithm does guarantee that when $\alpha_1$ elements are replicated in a plane on $\alpha_0$ elements, the maximum blocksize does not exceed the sum of the blocksizes of the planes on $\alpha_0$ and $\alpha_1$ elements. However, the scaling formula $91+73$ leads to maximum blocksize $20 > 10+9$ in 2329 of 2500 trials; formula $133+91$ leads to blocksize $23 > 12+10$ in 16 of 2500 trials; and formula $183+133$ leads to blocksize $27 > 14+12$ in 155 of 2500 trials. Hence, as described, the algorithm can fail even to ensure that the blocksize does not exceed the sum of the blocksizes of the planes whose numbers of elements appear in the scaling formula.

We modified the greedy strategy in order to improve its performance. A simple exchange heuristic is to examine the effect of replacing one of the replicated elements by one of the elements not yet replicated. We examined the number of blocks of maximum length before and after such a replacement, and if the number of such blocks did not increase, we carried out the replacement. Potential replacements are selected randomly, and the process repeated until no decrease in the number of maximum length blocks has been observed for some fixed number of trials (in our tests, for 10 000 trials). We tested this additional heuristic against the basic greedy method of [29] on PG$(2,8)$, and found that it makes an observable improvement. For example, in 50 executions of the two methods, the greedy method obtains an average maximum blocksize of 11.24 for scaling formula $73 + 7$, while the exchange heuristic improves this to 11.00. For $73 + 21$, greedy obtains average maximum blocksize 13.14 but the exchange heuristic obtains 13.00. For $73 + 57$, greedy obtains average maximum blocksize 17.82 but exchange obtains 17.00. The effectiveness of the exchange heuristic indicates that the greedy strategy is, perhaps, not focussing sufficiently on the proliferation of maximum length blocks. However, we do not expect simple heuristics to lead to the optimum solution with any regularity. Moreover, the addition of further heuristics has an adverse effect on the computation time to produce the covering.

## 3. (*k*, *n*)-arcs in projective planes

It is natural to ask whether there is an efficient algorithm for selecting elements to replicate so as to ensure that the maximum blocksize does not exceed the sum of the blocksizes of the planes whose numbers of elements appear in the scaling formula. We devise a very simple algorithm to ensure this next. Consider a phase in which $\alpha_i = x^2+x+1$ elements are to be chosen for replication in a base design on $\alpha_0 = q^2+q+1$ elements, i.e., PG$(2,q)$. We suppose that $x < q$, for otherwise all elements are to be replicated in this phase. We begin by selecting at random an element $z$ of PG$(2,q)$, and finding $x+1$ blocks $B_0,\ldots,B_x$ each containing $z$. For $0 \leqslant i \leqslant x$, let $C_i$ be a random set of $x+1$ elements of $B_i$, including $z$. Then we replicate the $x(x+1)+1$ elements in $\bigcup_{i=0}^{x} C_i$. Evidently each block containing $z$ has at most $x+1$ of its elements replicated. A block not containing $z$ intersects each block $B_0,\ldots,B_x$ in one element, and hence contains at most $x+1$ of the replicated elements. It follows that no blocksize increases by more than $x+1$ in this phase. Indeed, one can do better. When $x \leqslant q$, if one chooses $x+1$ elements in $C_i$ *not* including $z$, then $(x+1)^2$ elements can be replicated while increasing the maximum blocksize by at most $x+1$.

An apparently harder question is to determine the minimum increase in the maximum blocksize. For this purpose, there is no compelling reason to restrict the entries in the scaling formula, except of course $\alpha_0$, to be numbers of elements in a projective plane. Henceforth, we relax the requirement on a scaling formula so that $\alpha_0$ be the number of elements in a projective plane, and that $\alpha_1,\ldots,\alpha_t$ be positive integers satisfying $\alpha_{i+1} \leqslant \alpha_i$ for $0 \leqslant i < t$. We require further design theoretic notation.

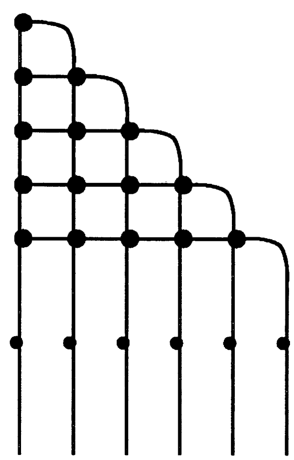
A $(k,n)$-*arc* in a projective plane of order $q$ is a nonempty set $K$ of $k$ elements such that $n$ is the maximum number of elements in $K$ that appear together on a block. A $(k,2)$-arc is a $k$-*arc*. The existence of $(k,n)$-arcs has been extensively studied, but their importance here is that the maximum number $m_n(q)$ of elements in a $(k,n)$-arc in PG$(2,q)$ is precisely the same as the maximum number of elements that can be replicated without increasing the maximum blocksize by more than $n$.

Barlotti [2] established that $m_n(q) \leqslant (n-1)(q+1)+1$. A simple computation establishes that when PG$(2,q)$ contains a $(k,n)$-arc whose size meets this bound, replicating the elements of the arc yields equality in the asymptotic bound of Füredi [14] discussed earlier. Unfortunately, the determination of $m_n(q)$ is a very difficult problem in finite geometry that remains far from settled [17–19]. Except when $n = q+1$, equality in Barlotti's bound can only be achieved when $n$ is a divisor of $q$ [2], and is achieved in two *trivial cases*: when $n = 1$ (by a single element), and when $n = q$ by all elements not lying on a fixed block. When $q$ is a second or higher power of a prime, nontrivial arcs meeting Barlotti's bound *always* exist when $q$ is a power of 2 and $n$ is a divisor of $q$ [13]. However, in a recent breakthrough it has been shown that they *never* exist when $q$ is a power of an odd prime [1].

When $m_n(q)$ does not realize Barlotti's bound, extensive research has attempted to obtain lower and upper bounds, and specific exact values; as an introduction to the extensive literature here, we suggest [3,15,16,24,26] and the surveys [17,19]. Each lower bound can lead to a replication scheme for producing a covering, and each upper bound establishes a limit on how well such a replication scheme can do.

We consider one specific example of developing a replication scheme using $(k,n)$-arcs. In 2500 trials on the scaling formula $183 + 73$, every single trial yields a maximum blocksize of $22 = 14 + 8$. However, $\mathrm{PG}(2,13)$ has a $(79,7)$-arc, and hence replicating 73 of the 79 elements in the arc yields a covering with maximum blocksize 21. Naturally, the existence of the $(79,7)$-arc does not provide a simple technique for finding it in order to determine which elements to replicate. To generalize this example, and to establish that the required arcs are easily found, we recall some well known results [18]. When $q$ is even, $m_2(q) = q + 2$ and the $(q + 2)$-arc is termed a *hyperoval.* A $(q + 1)$-arc is termed an *oval*, and when $q$ is odd, $m_2(q) = q + 1$.

$\mathrm{PG}(2,q)$, given as the difference set $(0,b_1,\dots,b_q)$, contains an oval on the elements $\{0,q^2+q+1-b_1,\dots,q^2+q+1-b_q\}$. Given $\mathrm{PG}(2,q)$ as the design $(V,\mathscr{B})$, the *dual* is a set system with elements $\{x_B\colon B\in\mathscr{B}\}$ and blocks $\mathscr{D}=\{\{x_B\colon y\in B\in\mathscr{B}\}\colon y\in V\}$. This notation can be more simply interpreted as interchanging the roles of blocks and elements. The dual of a projective plane is a projective plane, and the dual of $\mathrm{PG}(2,q)$ is again $\mathrm{PG}(2,q)$. The dual of a $k$-arc is a set of $k$ blocks, so that every element of the plane lies on at most two blocks in the dual $k$-arc. Since the dual is again a plane, every pair of blocks intersect. Hence, elements can be classified as *corners* that lie on two blocks of the dual arc, *covered elements* that lie on one, and *exterior elements* that lie on none. Next is depicted a dual 6-arc.



Every block meets the points on the blocks of a dual $(2\ell-1)$-arc in at least $\ell$ elements, since it meets each of the $2\ell-1$ blocks in an element, and can meet two blocks together only at a corner. Now, as an example, PG$(2,13)$ has an 13-arc (part of the 14-arc forming an oval), and so has a dual 13-arc. There are 78 corner elements, 26 covered elements, and 79 exterior elements, and these last form the (79,7)-arc mentioned above. In general, a dual $(2\ell-1)$-arc in PG$(2,q)$ has $\binom{2\ell-1}{2}$ corners, $(2\ell-1)(q+3-2\ell)$ covered elements, and $q^2+q+1-(2\ell-1)(q+2-\ell)$ exterior elements, and hence gives a $(q^2+q+1-(2\ell-1)(q+2-\ell), q+1-\ell)$-arc in PG$(2,q)$. Often one can improve upon this basic strategy by finding a dual $k$-arc for which no block meets $\ell-1$ corners. Indeed if each block not in the dual $(2\ell-1)$-arc meets at most $c$ corners, then the $x$ exterior elements form an $(x, q+1-(2\ell-1)+c)$-arc. When $c=2$, Ling and Colbourn [23] call this a *scattering* dual arc, but only some sporadic computational results are available.

This short discussion of $(k,n)$-arcs and their application is not intended to exhaust their uses in the construction of coverings for the network design problem, but rather to indicate two things. First of all, the determination of the optimal coverings appears likely to be very difficult, involving the exact determination of $m_n(q)$. Secondly, on a brighter note, existing techniques for producing large $(k,n)$-arcs appear to be very useful in obtaining practical solutions, providing a technique that is at once more accurate, and computationally simpler, than the greedy method of [29].

## 4. Difference covers

Previous efforts on this network design problem have not addressed the question of how to proceed when the degree constraint $r$ is not one more than the order of a projective plane, except to suggest that the degree constraint be reduced until this constraint is met. Consider, for example, the case when $r=7$. There is no plane of order 6, and hence the plane PG$(2,5)$ can be used. In this case, if $v=39$ and $r=7$, the scaling formula $31+8$ leads to maximum blocksize 9, while the scaling formula $21+17$ leads to maximum blocksize 10. However, there is a covering on 39 elements with replication number 7 and blocksize 7 [28], and hence in this case replication of elements in planes does not appear to lead to the best solution. For this reason, we mention a less well studied generalization of difference sets that can lead to (slightly) smaller blocksizes for certain degree constraints.

A *difference cover* modulo $v$ of *order* $q$, $D=\{d_0,\ldots,d_q\}$, has the property that $\{d_i-d_j\colon 0\leqslant i,j\leqslant q \text{ and } i\neq j\}$, arithmetic modulo $v$, contains every nonzero integer in $\mathbb{Z}_v$. Hence, every nonzero difference arises at least once as the difference modulo $v$ of two elements in $D$. When $v=q^2+q+1$, a difference cover is a difference set. However, while difference sets only exist for certain values of $q$, difference covers exist for every value of $q$. Of course, the price one pays is that the number of elements $v$ is less than $q^2+q+1$ in general. Now, adding each integer $i$ to the elements of $D$ in turn, we produce $v$ blocks forming a covering with blocksize $q+1$ and replication number $q+1$. Wiedemann [28] gives a difference cover modulo 39 of order 6, which provides the illustration given above. He also presents a table of the smallest order difference cover modulo $v$ for each value of $v \leqslant 133$. Unfortunately, these computational results are not at present accompanied by a useful theory. A result of Wichmann [11,27] establishes that a difference cover modulo $v$ exists with order at most $\sqrt{\frac{3}{2}}\sqrt{v}+3$, but this bound is not sufficiently tight to guarantee that difference covers exist which yield better coverings than those obtained by simply employing a projective plane with smaller replication number. Nevertheless, for certain small replication numbers such as 7 (a difference cover modulo 39), and 11 (a difference cover modulo 95 [28]), it appears that difference covers can improve upon the use of planes. However, in this case, the structure of the covers does not share the algebraic structure of the desarguesian planes, and so one ought not to expect to find simple strategies for determining elements to replicate. In this case, the greedy method of Yener et al. [29] appears to be an excellent heuristic technique.

## 5. Conclusions

Producing coverings for the network design problem of Yener et al. [29] is intimately tied to the structure of projective planes by the bound of Füredi, and the structure of optimal coverings is closely related to the rich algebraic and combinatorial structure of the planes. While the greedy method does not appear to lead to optimal solutions, in general, one can exploit known results on $(k,n)$-arcs in projective planes to reach the optimum in some cases, and to improve upon the greedy strategy in others. The improvement is both in terms of the parameters of the covering achieved, and in terms of the computational difficulty of producing the covering. Finally, we reiterate that the exact determination of parameters for an optimal covering is likely very difficult, as it appears to require the solution of a number of well studied, but still open, problems. Bierbrauer [8] examines a related problem on assigning weights to elements of affine planes, and he [9] establishes useful connections from the coverings from projective planes to binary codes, which support these observations.

## Acknowledgements

Thanks to Sanjoy Baruah for bringing the paper [29] to my attention, and for very helpful discussions. Thanks also to Jeff Dinitz and Don Kreher.

## References

[1] S. Ball, A. Blokhuis, F. Mazzocca, Maximal arcs in Desarguesian planes of odd order do not exist, Combinatorica 17 (1997) 31–41.
[2] A. Barlotti, Su $\{k,n\}$-archi di un piano lineare finito, Boll. Un. Mat. Ital. 11 (1956) 553–556.
[3] A. Barlotti, Some topics in finite geometrical structures, Report 439, Institute of Statistics, University of North Carolina, 1965.
[4] J.C. Bermond, J. Bond, M. Paoli, C. Peyrat, Graphs and interconnection networks: diameter and vulnerability, in: E.K. Lloyd (Ed.), Surveys in Combinatorics 1983, Cambridge University Press, Cambridge, 1983, pp. 1–30.

[5] J.C. Bermond, J. Bond, J.F. Saclé, Large hypergraphs of diameter 1, Graph Theory Combinatorics, Proceedings Colloquim, Cambridge, 1984, pp. 19–28.
[6] J.-C. Bermond, F.Ö. Ergincan, Bus interconnection networks, Discrete Appl. Math. 68 (1996) 1–15.
[7] Th. Beth, D. Jungnickel, H. Lenz, Design Theory, Cambridge University Press, Cambridge, 1986.
[8] J. Bierbrauer, Small islands, Extremal Problems for Finite Sets (Visegrád, 1991), Bolyai Soc. Math. Stud., vol. 3, János Bolyai Math. Soc., Budapest, 1994, pp. 93–110.
[9] J. Bierbrauer, Three-dimensional codes and a network problem, preprint, 1999.
[10] C.J. Colbourn, J.H. Dinitz (Eds.), CRC Handbook of Combinatorial Designs, CRC Press, Boca Raton, FL, 1996.
[11] C.J. Colbourn, A.C.H. Ling, Quorums from difference covers, Inform. Process. Lett. 75 (2000) 9–12.
[12] C.J. Colbourn, P.C. van Oorschot, Applications of combinatorial designs in computer science, ACM Comput. Surveys 21 (1989) 223–250.
[13] R.H.F. Denniston, Some maximal arcs in finite projective planes, J. Combin. Theory 6 (1969) 317–319.
[14] Z. Füredi, Maximum degree and fractional matchings in uniform hypergraphs, Combinatorica 1 (1981) 155–162.
[15] R. Hill, Some problems concerning $(k,n)$-arcs in finite projective planes, Rend. Semin. Mat. Brescia 7 (1984) 367–383.
[16] R. Hill, J.R.M. Mason, On $(k,n)$-arcs and the falsity of the Lunelli-Sce conjecture, Finite Geometries and Designs, Cambridge University Press, Cambridge, 1982, pp. 153–168.
[17] J.W.P. Hirschfeld, Maximum sets in finite projective planes, in: E.K. Lloyd (Ed.), Surveys in Combinatorics 1983, Cambridge University Press, Cambridge, 1983, pp. 55–76.
[18] J.W.P. Hirschfeld, Projective Geometries Over Finite Fields, 2nd Edition, Oxford University Press, Oxford, 1998.
[19] J.W.P. Hirschfeld, L. Storme, The packing problem in statistics, coding theory and finite projective spaces, J. Statist. Planning Inference 72 (1998) 355–380.
[20] D.R. Hughes, F.C. Piper, Projective Planes, Springer, New York, 1973.
[21] J. Kilian, S. Kipnis, C.E. Leiserson, The organization of permutation architectures with bussed interconnections, IEEE Trans. Comput. 39 (1990) 1346–1358.
[22] C.W.H. Lam, L. Thiel, S. Swiercz, The non-existence of finite projective planes of order 10, Canad. J. Math. 41 (1989) 1117–1123.
[23] A.C.H. Ling, C.J. Colbourn, Deleting lines in projective planes, Ars Combin. 50 (1998) 129–138.
[24] J.R.M. Mason, On the maximum sizes of certain $(k,n)$-arcs in finite projective geometries, Math. Proc. Cambridge Philos. Soc. 91 (1982) 153–170.
[25] M.D. Mickunas, Using projective geometry to design bus connection networks, in: Proceedings of Workshop on Interconnection Networks for Parallel and Distributed Processing, 1980, pp. 47–55.
[26] W.C. Waterhouse, Abelian varieties over finite fields, Ann. Sci. École Norm. Sup. 2 (1969) 521–560.
[27] B.A. Wichmann, A note on restricted difference sets, J. London Math. Soc. 38 (1963) 465–466.
[28] D. Wiedemann, Cyclic difference covers through 133, Congr. Numer. 90 (1992) 181–185.
[29] B. Yener, Y. Ofek, M. Yung, Combinatorial design of congestion-free networks, IEEE/ACM Trans. Networking 5 (1997) 989–1000.